# Table of Contents – Part III

## Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. A)

A Security Requirement Management Database Based on ISO/IEC 15408

*Shoichi Morimoto, Daisuke Horie, Jingde Cheng* ............................... 1

Development of Committee Neural Network for Computer Access Security System

*A. Sermet Anagun* ............................... 11

C-TOBI-Based Pitch Accent Prediction Using Maximum-Entropy Model

*Byeongchang Kim, Gary Geunbae Lee* ............................... 21

Design and Fabrication of Security and Home Automation System

*Eung Soo Kim, Min Sung Kim* ............................... 31

PGNIDS (Pattern-Graph Based Network Intrusion Detection System) Design

*Byung-kwan Lee, Seung-hae Yang, Dong-Hyuck Kwon,
Dai-Youn Kim* ............................... 38

Experiments and Hardware Countermeasures on Power Analysis Attacks

*ManKi Ahn, HoonJae Lee* ............................... 48

Information System Modeling for Analysis of Propagation Effects and Levels of Damage

*InJung Kim, YoonJung Chung, YoungGyo Lee, Eul Gyu Im,
Dongho Won* ............................... 54

A Belt-Zone Method for Decreasing Control Messages in Ad Hoc Networks

*Youngrag Kim, JaeYoun Jung, Seunghwan Lee, Chonggun Kim* ............................... 64

A VLSM Address Management Method for Variable IP Subnetting

*SeongKwon Cheon, DongXue Jin, ChongGun Kim* ............................... 73

SDSEM: Software Development Success Evolution Model

*Haeng-Kon Kim, Sang-Yong Byun* ............................... 84
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Robust Routing Protocol by a Substitute Local Path in Ad Hoc Networks</td>
<td>Mary Wu, SangJoon Jung, Seunghwan Lee, Chonggun Kim</td>
<td>93</td>
</tr>
<tr>
<td>Power Efficient Wireless LAN Using 16-State Trellis-Coded Modulation for Infrared Communications</td>
<td>Hae Geun Kim</td>
<td>104</td>
</tr>
<tr>
<td>Ontology-Based Information Search in the Real World Using Web Services</td>
<td>Hyun-Suk Hwang, Kyoo-Seok Park, Chang-Soo Kim</td>
<td>125</td>
</tr>
<tr>
<td>An Active Node Set Maintenance Scheme for Distributed Sensor Networks</td>
<td>Tae-Young Byun, Minsu Kim, Sungho Hwang, Sung-Eok Jeon</td>
<td>134</td>
</tr>
<tr>
<td>Intelligent Information Search Mechanism Using Filtering and NFC Based on Multi-agents in the Distributed Environment</td>
<td>Subong Yi, Bobby D. Gerardo, Young-Seok Lee, Jaewan Lee</td>
<td>144</td>
</tr>
<tr>
<td>Network Anomaly Behavior Detection Using an Adaptive Multiplex Detector</td>
<td>Misun Kim, Minsoo Kim, JaeHyun Seo</td>
<td>154</td>
</tr>
<tr>
<td>Applying Product Line to the Embedded Systems</td>
<td>Haeng-Kon Kim</td>
<td>163</td>
</tr>
<tr>
<td>Enhanced Fuzzy Single Layer Learning Algorithm Using Automatic Tuning of Threshold</td>
<td>Kwang-Baek Kim, Byung-Kwan Lee, Soon-Ho Kim</td>
<td>172</td>
</tr>
<tr>
<td>Optimization of Location Management in the Distributed Location-Based Services Using Collaborative Agents</td>
<td>Romeo Mark A. Mateo, Jaewan Lee, Hyunho Yang</td>
<td>178</td>
</tr>
<tr>
<td>Design of H.264/AVC-Based Software Decoder for Mobile Phone</td>
<td>Hyung-Su Jeon, Hye-Min Noh, Cheol-Jung Yoo, Ok-Bae Chang</td>
<td>188</td>
</tr>
<tr>
<td>Transforming a Legacy System into Components</td>
<td>Haeng-Kon Kim, Youn-Ky Chung</td>
<td>198</td>
</tr>
</tbody>
</table>
Pseudorandom Number Generator Using Optimal Normal Basis  
*Injoo Jang, Hyeong Seon Yoo* ................................................. 206

Efficient Nonce-Based Authentication Scheme Using Token-Update  
*Wenbo Shi, Hyeong Seon Yoo* .................................................... 213

An Efficient Management of Network Traffic Performance Using Framework-Based Performance Management Tool  
*Seong-Man Choi, Cheol-Jung Yoo, Ok-Bae Chang* ......................... 222

A Prediction Method of Network Traffic Using Time Series Models  
*Sangjoon Jung, Chonggun Kim, Younky Chung* ............................... 234

An Obstacle Avoidance Method for Chaotic Robots Using Angular Degree Limitations  
*Youngchul Bae, MalRey Lee, Thomas M. Gatton* ............................ 244

Intersection Simulation System Based on Traffic Flow Control Framework  
*Chang-Sun Shin, Dong-In Ahn, Hyun Yoe, Su-Chong Joo* .................. 251

A HIICA(Highly-Improved Intra CA) Design for M-Commerce  
*Byung-kwan Lee, Chang-min Kim, Dae-won Shin, Seung-hae Yang* ......... 261

Highly Reliable Synchronous Stream Cipher System for Link Encryption  
*HoonJae Lee* .............................................................................. 269

Recognition of Concrete Surface Cracks Using ART2-Based Radial Basis Function Neural Network  
*Kwang-Baek Kim, Hwang-Kyu Yang, Sang-Ho Ahn* ............................ 279

Hybrid Image Mosaic Construction Using the Hierarchical Method  
*Oh-Hyung Kang, Ji-Hyun Lee, Yang-Won Rhee* ............................... 287

**Workshop on Applied Cryptography and Information Security (ACIS 2006)**

Public Key Encryption with Keyword Search Based on K-Resilient IBE  
*Dalia Khader* ............................................................................. 298

A Generic Construction of Secure Signatures Without Random Oracles  
*Jin Li, Yuen-Yan Chan, Yanming Wang* .......................................... 309
A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption  
*David Galindo* .......................................................... 318

Traceable Signature: Better Efficiency and Beyond  
*He Ge, Stephen R. Tate* .................................................. 327

On the TYS Signature Scheme  
*Marc Joye, Hung-Mei Lin* ................................................. 338

Efficient Partially Blind Signatures with Provable Security  
*Qianhong Wu, Willy Susilo, Yi Mu, Fanguo Zhang* .................. 345

A Framework for Robust Group Key Agreement  
*Jens-Matthias Bohli* ....................................................... 355

BGN Authentication and Its Extension to Convey Message Commitments  
*Yuen-Yan Chan, Jin Li* ................................................... 365

New Security Problem in RFID Systems “Tag Killing”  
*Dong-Guk Han, Tsuyoshi Takagi, Ho Won Kim, Kyo Il Chung* .... 375

A Model for Security Vulnerability Pattern  
*Hyungwoo Kang, Kibom Kim, Soonjwa Hong, Dong Hoon Lee* .... 385

A New Timestamping Scheme Based on Skip Lists  
*Kaouthar Blibech, Alban Gabillon* ...................................... 395

A Semi-fragile Watermarking Scheme Based on SVD and VQ Techniques  
*Hsien-Chu Wu, Chuan-Po Yeh, Chwei-Shyong Tsai* .................. 406

New Constructions of Universal Hash Functions Based on Function Sums  
*Khoongming Khoo, Swee-Huay Heng* .................................... 416

Analysis of Fast Blockcipher-Based Hash Functions  
*Martin Stanek* .............................................................. 426

Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms  
*Sourav Mukhopadhyay, Palash Sarkar* .................................. 436

Provable Security for an RC6-like Structure and a MISTY-FO-like Structure Against Differential Cryptanalysis  
*Changhoon Lee, Jongsung Kim, Jaechul Sung, Seokhie Hong, Sangjin Lee* .................................................. 446
Design and Implementation of an FPGA-Based 1.452-Gbps Non-pipelined AES Architecture
Ignacio Algredo-Badillo, Claudia Feregrino-Uribe, René Cumplido ... 456

Workshop on Internet Communications Security (WICS 2006)

Security Weaknesses in Two Proxy Signature Schemes
Jiqiang Lu ................................................................. 466

A Proposal of Extension of FMS-Based Mechanism to Find Attack Paths
Byung-Ryong Kim, Ki-Chang Kim ........................................ 476

Comparative Analysis of IPv6 VPN Transition in NEMO Environments
Hyung-Jin Lim, Dong-Young Lee, Tai-Myoung Chung ................. 486

A Short-Lived Key Selection Approach to Authenticate Data Origin of Multimedia Stream
Namhi Kang, Younghan Kim .............................................. 497

Weakest Link Attack on Single Sign-On and Its Case in SAML V2.0 Web SSO
Yuen-Yan Chan ............................................................. 507

An Inter-domain Key Agreement Protocol Using Weak Passwords
Youngsook Lee, Junghyun Nam, Dongho Won ............................ 517

A Practical Solution for Distribution Rights Protection in Multicast Environments
Josep Pegueroles, Marcel Fernández, Francisco Rico-Novella,
Miguel Soriano ............................................................ 527

Audit-Based Access Control in Nomadic Wireless Environments
Francesco Palmieri, Ugo Fiore ........................................... 537

Workshop on Optimization: Theories and Applications (OTA 2006)

Cost – Time Trade Off Models Application to Crashing Flow Shop Scheduling Problems
Morteza Bagherpour, Siamak Noori, S. Jafar Sadjadi .................. 546
The ASALB Problem with Processing Alternatives Involving Different Tasks: Definition, Formalization and Resolution  
Liliana Capacho, Rafael Pastor ................................. 554

Satisfying Constraints for Locating Export Containers in Port Container Terminals  
Kap Hwan Kim, Jong-Sool Lee ................................. 564

A Price Discrimination Modeling Using Geometric Programming  
Seyed J. Sadjadi, M. Ziaee ................................. 574

Hybrid Evolutionary Algorithms for the Rectilinear Steiner Tree Problem Using Fitness Estimation  
Byounghak Yang ................................. 581

Data Reduction for Instance-Based Learning Using Entropy-Based Partitioning  
Seung-Hyun Son, Jae-Yearn Kim ................................. 590

Coordinated Inventory Models with Compensation Policy in a Three Level Supply Chain  
Jeong Hun Lee, Il Kyeong Moon ................................. 600

Using Constraint Satisfaction Approach to Solve the Capacity Allocation Problem for Photolithography Area  
Shu-Hsing Chung, Chun-Ying Huang, Amy Hsin-I Lee ................................. 610

Scheduling an R&D Project with Quality-Dependent Time Slots  
Mario Vanhoucke ................................. 621

The Bottleneck Tree Alignment Problems  
Yen Hung Chen, Chuan Yi Tang ................................. 631

Performance Study of a Genetic Algorithm for Sequencing in Mixed Model Non-permutation Flowshops Using Constrained Buffers  
Gerrit Färber, Anna M. Coves Moreno ................................. 638

Optimizing Relative Weights of Alternatives with Fuzzy Comparative Judgment  
Chung-Hsing Yeh, Yu-Hern Chang ................................. 649

Model and Solution for the Multilevel Production-Inventory System Before Ironmaking in Shanghai Baoshan Iron and Steel Complex  
Guoli Liu, Lixin Tang ................................. 659
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Coordination Algorithm for Deciding Order-Up-To Level of a Serial</td>
<td>Kung-Jeng Wang, Wen-Hai Chih, Ken Hwang</td>
<td>668</td>
</tr>
<tr>
<td>Supply Chain in an Uncertain Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimization of Performance of Genetic Algorithm for 0-1 Knapsack</td>
<td>A.S. Anagun, T. Sarac</td>
<td>678</td>
</tr>
<tr>
<td>Problems Using Taguchi Method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Truck Dock Assignment Problem with Time Windows and Capacity</td>
<td>Andrew Lim, Hong Ma, Zhaowei Miao</td>
<td>688</td>
</tr>
<tr>
<td>Constraint in Transshipment Network Through Crossdocks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An Entropy Based Group Setup Strategy for PCB Assembly</td>
<td>In-Jae Jeong</td>
<td>698</td>
</tr>
<tr>
<td>Cross-Facility Production and Transportation Planning Problem with</td>
<td>Sandra Duni Eksioglu, Mingzhou Jin</td>
<td>708</td>
</tr>
<tr>
<td>Perishable Inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Unified Framework for the Analysis of M/G/1 Queue Controlled by</td>
<td>Ho Woo Lee, Se Won Lee, Won Ju Seo, Sahng Hoon Cheon, Jongwoo Jeon</td>
<td>718</td>
</tr>
<tr>
<td>Workload</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabu Search Heuristics for Parallel Machine Scheduling with</td>
<td>Sang-Il Kim, Hyun-Seon Choi, Dong-Ho Lee</td>
<td>728</td>
</tr>
<tr>
<td>Sequence-Dependent Setup and Ready Times</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Maximum Integer Multiterminal Flow Problem</td>
<td>Cédric Bentz</td>
<td>738</td>
</tr>
<tr>
<td>Routing with Early Ordering for Just-In-Time Manufacturing Systems</td>
<td>Mingzhou Jin, Kai Liu, Burak Eksioglu</td>
<td>748</td>
</tr>
<tr>
<td>A Variant of the Constant Step Rule for Approximate Subgradient</td>
<td>Eugenio Mijangos</td>
<td>757</td>
</tr>
<tr>
<td>Methods over Nonlinear Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On the Optimal Buffer Allocation of an FMS with Finite In-Process</td>
<td>Soo-Tae Kwon</td>
<td>767</td>
</tr>
<tr>
<td>Buffers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimization Problems in the Simulation of Multifactor Portfolio</td>
<td>Wanmo Kang, Kyungsik Lee</td>
<td>777</td>
</tr>
<tr>
<td>Credit Risk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Two-Server Network Disconnection Problem
*Byung-Cheon Choi, Sung-Pil Hong*

785

### One-Sided Monge TSP Is NP-Hard
*Vladimir Deineko, Alexander Tiskin*

793

### On Direct Methods for Lexicographic Min-Max Optimization
*Wlodzimierz Ogryczak, Tomasz Śliwiński*

802

### Multivariate Convex Approximation and Least-Norm Convex Data-Smoothing
*Alex Y.D. Siem, Dick den Hertog, Aswin L. Hoffmann*

812

### Linear Convergence of Tatonnement in a Bertrand Oligopoly
*Guillermo Gallego, Woonghee Tim Huh, Wanmo Kang, Robert Phillips*

822

### Design for Using Purpose of Assembly-Group
*Hak-Soo Mok, Chang-Hyo Han, Chan-Hyoung Lim, John-Hee Hong, Jong-Rae Cho*

832

### A Conditional Gaussian Martingale Algorithm for Global Optimization
*Manuel L. Esquivel*

841

### Finding the Number of Clusters Minimizing Energy Consumption of Wireless Sensor Networks
*Hyunsoo Kim, Hee Yong Youn*

852

### A Two-Echelon Deteriorating Production-Inventory Newsboy Model with Imperfect Production Process
*Hui-Ming Wee, Chun-Jen Chung*

862

### Mathematical Modeling and Tabu Search Heuristic for the Traveling Tournament Problem
*Jin Ho Lee, Young Hoon Lee, Yun Ho Lee*

875

### An Integrated Production-Inventory Model for Deteriorating Items with Imperfect Quality and Shortage Backordering Considerations
*H.M. Wee, Jonas C.P. Yu, K.J. Wang*

885

### A Clustering Algorithm Using the Ordered Weight Sum of Self-Organizing Feature Maps
*Jong-Sub Lee, Maing-Kyu Kang*

898
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Optimization of the Scenario Generation and Portfolio Selection Problems</td>
<td>Panos Parpas, Berc Rüstern</td>
<td>908</td>
</tr>
<tr>
<td>A Generalized Fuzzy Optimization Framework for R&amp;D Project Selection Using Real Options Valuation</td>
<td>E. Ertugrul Karsak</td>
<td>918</td>
</tr>
<tr>
<td>Supply Chain Network Design and Transshipment Hub Location for Third Party Logistics Providers</td>
<td>Seungwoo Kwon, Kyungdo Park, Chulung Lee, Sung-Shick Kim, Hak-Jin Kim, Zhong Liang</td>
<td>928</td>
</tr>
<tr>
<td>A Group Search Optimizer for Neural Network Training</td>
<td>S. He, Q.H. Wu, J.R. Saunders</td>
<td>934</td>
</tr>
<tr>
<td>Application of Two-Stage Stochastic Linear Program for Portfolio Selection Problem</td>
<td>Kuo-Hwa Chang, Huifen Chen, Ching-Fen Lin</td>
<td>944</td>
</tr>
<tr>
<td><strong>General Tracks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hierarchical Clustering Algorithm Based on Mobility in Mobile Ad Hoc Networks</td>
<td>Sulyun Sung, Yuhwa Seo, Yongtae Shin</td>
<td>954</td>
</tr>
<tr>
<td>Static Analysis Based Software Architecture Recovery</td>
<td>Jiang Guo, Yuechong Liao, Raj Pamula</td>
<td>974</td>
</tr>
<tr>
<td>A First Approach to a Data Quality Model for Web Portals</td>
<td>Angelica Caro, Coral Calero, Ismael Caballero, Mario Piattini</td>
<td>984</td>
</tr>
<tr>
<td>Design for Environment-Friendly Product</td>
<td>Hak-Soo Mok, Jong-Rae Cho, Kwang-Sup Moon</td>
<td>994</td>
</tr>
<tr>
<td>Performance of HECC Coprocessors Using Inversion-Free Formulae</td>
<td>Thomas Wollinger, Guido Bertoni, Luca Breveglieri, Christof Paar</td>
<td>1004</td>
</tr>
<tr>
<td>Metrics of Password Management Policy</td>
<td>Carlos Villarrubia, Eduardo Fernández-Medina, Mario Piattini</td>
<td>1013</td>
</tr>
</tbody>
</table>
Using UML Packages for Designing Secure Data Warehouses
   Rodolfo Villarroel, Emilio Soler, Eduardo Fernández-Medina,
   Juan Trujillo, Mario Piattini .............................................................. 1024

Practical Attack on the Shrinking Generator
   Pino Caballero-Gil, Amparo Fuster-Sabater ........................................... 1035

A Comparative Study of Proposals for Establishing Security
Requirements for the Development of Secure Information Systems
   Daniel Mellado, Eduardo Fernández-Medina, Mario Piattini ...................... 1044

Stochastic Simulation Method for the Term Structure Models with Jump
   Kisoeb Park, Moonseong Kim, Seki Kim ................................................... 1054

The Ellipsoidal $l_p$ Norm Obnoxious Facility Location Problem
   Yu Xia ........................................................................................................... 1064

On the Performance of Recovery Rate Modeling
   J. Samuel Baixauli, Susana Alvarez ......................................................... 1073

Using Performance Profiles to Evaluate Preconditioners for Iterative
Methods
   Michael Lazzareschi, Tzu-Yi Chen ............................................................ 1081

Multicast $\omega$-Trees Based on Statistical Analysis
   Moonseong Kim, Young-Cheol Bang, Hyunseung Choo ................................. 1090

The Gateways Location and Topology Assignment Problem in
Hierarchical Wide Area Networks: Algorithms and Computational
Results
   Przemyslaw Ryba, Andrzej Kasprzak ......................................................... 1100

Developing an Intelligent Supplier Chain System Collaborating with
Customer Relationship Management
   Gye Hang Hong, Sung Ho Ha ................................................................. 1110

The Three-Criteria Servers Replication and Topology Assignment
Problem in Wide Area Networks
   Marcin Markowski, Andrzej Kasprzak ...................................................... 1119

An Efficient Multicast Tree with Delay and Delay Variation Constraints
   Moonseong Kim, Young-Cheol Bang, Jong S. Yang,
   Hyunseung Choo ............................................................................................ 1129

Algorithms on Extended $(\delta, \gamma)$-Matching
   Inbok Lee, Raphaël Clifford, Sung-Ryul Kim ............................................. 1137
SOM and Neural Gas as Graduated Nonconvexity Algorithms
Ana I. González, Alicia D’Anjou, M. Teresa García-Sebastián,
Manuel Graña ............................................................... 1143

Analysis of Multi-domain Complex Simulation Studies
James R. Gattiker, Earl Lawrence, David Higdon ..................... 1153

A Fast Method for Detecting Moving Vehicles Using Plane Constraint
of Geometric Invariance
Dong-Joong Kang, Jong-Eun Ha, Tae-Jung Lho ......................... 1163

Robust Fault Matched Optical Flow Detection Using 2D Histogram
Jaechoon Chon, Hyongsuk Kim ............................................ 1172

Iris Recognition: Localization, Segmentation and Feature Extraction
Based on Gabor Transform
Mohammadreza Noruzi, Mansour Vafadoost, M. Shahram Moin ..... 1180

Optimal Edge Detection Using Perfect Sharpening of Ramp Edges
Eun Mi Kim, Cherl Soo Pahk, Jong Gu Lee .............................. 1190

Eye Tracking Using Neural Network and Mean-Shift
Eun Yi Kim, Sin Kuk Kang .................................................. 1200

The Optimal Feature Extraction Procedure for Statistical Pattern
Recognition
Marek Kurzynski, Edward Puchala ....................................... 1210

A New Approach for Human Identification Using Gait Recognition
Murat Ekinci ................................................................. 1216

Author Index ............................................................... 1227